Competition, Speculative Risks, and IT Security Outsourcing

Asunur Cezar, Huseyin Cavusoglu, Srinivasan Raghunathan
The School of Management,
The University of Texas at Dallas
Richardson, TX 75083
{asunur.cezar,huseyin,sraghu}@utdallas.edu

Abstract

Information security management is becoming a more critical and, simultaneously, a challenging function for many firms. Even though many security managers are skeptical about outsourcing of IT security, others have cited reasons that are used for outsourcing of traditional IT functions for why security outsourcing is likely to increase. In this paper, we offer a novel explanation, based on competitive externalities associated with IT security, for firms' decisions to outsource IT security. We show that if competitive externalities are ignored, then a firm will outsource security if and only if the MSSP offers a quality (or a cost) advantage over in-house operations, which is consistent with the traditional explanation for security outsourcing. However, a higher quality is neither a prerequisite nor a guarantee for a firm to outsource security. The competitive risk environment and the nature of the security function outsourced, in addition to quality, determine firms' outsourcing decisions. If the reward from the competitor's breach is higher than the loss from own breach, then even if the likelihood of a breach is higher under the MSSP the expected benefit from the competitive demand externality may offset the loss from the higher likelihood of breaches, resulting in one or both firms outsourcing security. The incentive to outsource security monitoring is higher than that of infrastructure management because the MSSP can reduce the likelihood of breach on both firms and thus enhance the demand externality effect. The incentive to outsource security monitoring (infrastructure management) is higher (lower) if either the likelihood of breach on both firms is lower (higher) when security is outsourced or the benefit (relative to loss) from the externality is higher (lower). The benefit from the demand externality arising out of a security breach is higher when more of the customers that leave the breached firm switch to the non-breached firm.

March 2009

1. Introduction

Information security management is emerging as a critical business function, partly because of firms' increasing reliance on the Internet to conduct business and increasing regulatory requirements. Simultaneously, information security management is becoming more complex and challenging. Some of the reasons for this include changes in attack patterns over time (increased frequency, severity and sophistication of attacks); complex information technology (IT) environments consisting of multitudes of hardware, operating systems, application software, and distributed networks, each with its own vulnerabilities; shortage of security professionals with the required expertise; diverse security solutions from vendors; limited IT budgets; and demanding audit and regulatory requirements (e.g., Sarbanes Oxley (SOX), California Senate Bill No. 1386, Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accounting Act (HIPPA), Payment Card Industry Data Security Standard (PCI DSS), Basel II, among others). Outsourcing to Managed Security Service Providers (MSSP) has emerged as one of the key strategies to deal with the complexities of IT security management. The MSSP industry is relatively new, but analysts project significant growth in the MSSP industry. According to IDC, the value of U.S. managed security services market was approximately $1.3 billion in 2007, an increase of 19.6% over 2006; this figure is expected to reach $2.8 billion by 2012 (IDC 2008). Yankee Group estimated that the global spending on managed security services was approximately $4 billion in 2006. They projected managed security services market to grow at a compound annual rate of 14 percent from 2006 through 2010 (Palumbo, 2006). Frost and Sullivan expects managed security services market to exceed $6 billion by 2011 (Reed 2008). According to Gartner, in 2006, 60% of Fortune 500 enterprises had used an MSSP, and about 20% of enterprise firewalls were under remote monitoring or management (Gartner 2007). The range of services outsourced includes perimeter protection which includes managed services for firewalls, IDSs, VPNs, and other security infrastructure management, security event monitoring, incident management including emergency response and forensic analysis, and security consulting that includes vulnerability assessment, penetration testing, network architecture review, and compliance gap analysis.

Even though many security managers are skeptical about outsourcing of IT security (Messmer 2008, Ernst & Young's 2008 Global Information Security Survey), mainly due to the fear of losing control over sensitive information, industry analysts have cited cost savings, better protection, leveraging of expertise, economies of scale, compliance with laws, and liability transfer as the primary drivers for the outsourcing of information security functions (Wylder 2004, Ding et al. 2005a, Rowe 2007). Schneier (2008) noted that information security is part of IT infrastructure and "infrastructure is always outsourced." These reasons for IT security outsourcing suggest that practitioners and industry experts do not view IT security as different from traditional IT functions such as systems development, maintenance, help desk support, and data center operations, which are routinely outsourced. However, while IT security and traditional IT functions share many common risks, some of these risks are more significant in the IT security context. For instance, when the security of a firm is breached, the firm not only incurs losses related to recovery from the breach and from possible business disruptions, but may also lose customers to non-breached competitors if the breach is publicly revealed. Thus, the non-breached firm may stand to gain from the breached competitor. The recovery and business disruption-related costs are found in traditional IT failures. However, the cost (benefit) associated with loss (gain) of customers is not significant in traditional IT failures[1]. The risks involving traditional IT failures are in general non-speculative, which are those exogenous events from which only a loss can occur. However, because of competitive externalities, IT security may involve speculative risks, which are events from which *either* a profit or a loss can occur (Tarantino 2008).

One reason that IT security environment exhibits speculative risks is the competition between firms induced by security-sensitive customers that may switch from a firm that does not protect their information to another firm that does. The relative magnitudes of non-speculative and speculative components of information security breach risk are evident from the results of a recent Ponemon Institute study (Ponemon Institute 2007). The study found that the average total cost of a data breach, which

[1] The literature on traditional IT outsourcing does not suggest this risk as one of the reasons for firms' decisions to outsource, implying that this risk is not a significant factor in traditional IT failures.

included direct cost (such as free or discounted services offered, notification letters, phone calls and emails, and legal and auditing fees), lost productivity costs (such as the lost employee or contractor time diverted from other tasks to security breach related tasks), and customer opportunity costs which cover turnover of existing customers and increased difficulty in acquiring new customers was $197 for each breached customer record in 2007, an increase of 8% and 43% since 2006 and 2005, respectively. In the financial services industry, the cost per breached record was even higher at $239. The cost of lost business (due to customer churn) averaged 65% of the total cost (versus 54% in 2006) or $128 per breached record, and this figure increased at more than 30 percent, averaging $128 per breached record. The customer churn rate averaged 2.67% in 2007, an increase from 2.01% in 2006. The study reported that customers have not become accustomed to new data breaches, but, on the contrary, they are increasingly prone to terminate their business relationships due to security breaches. Further, results from the CSI Survey 2007 suggest that the burden of security breaches are often transferred to customers, thus enhancing customers' incentives to switch to another firm that is not breached. The empirical data related to risks associated with security breaches clearly suggest that analyzing IT security outsourcing decisions solely on the basis of non-competitive and non-speculative factors is incomplete.

Using a simple game theoretical model of two firms deciding to either perform in-house security management or outsource their IT security functions, we show that if competitive externalities are ignored, then a firm will outsource security if and only if the MSSP offers a quality (or a cost) advantage over in-house operations, which is consistent with the traditional explanation for security outsourcing. However, a higher quality is neither a prerequisite nor a guarantee for a firm to outsource security. The competitive risk environment and the nature of the security function outsourced, in addition to quality, determine firms' outsourcing decisions. If the reward from the competitor's breach is higher than the loss from own breach, then even if the likelihood of a breach is higher under the MSSP the expected benefit from the competitive demand externality may offset the loss from the higher likelihood of breaches, resulting in one or both firms outsourcing security. The incentive to outsource security monitoring is higher than that of infrastructure management because the MSSP can reduce the likelihood of breach on both firms and thus enhance the demand externality effect. The incentive to outsource security monitoring (infrastructure management) is higher (lower) if either the likelihood of breach on both firms is lower (higher) when security is outsourced or the benefit (relative to loss) from the externality is higher (lower). The benefit from the demand externality arising out of a security breach is higher when more of the customers that leave the breached firm switch to the non-breached firm.

The rest of the paper is organized as follows. In the next section, we review the vast research on general IT outsourcing and the limited research on IT security outsourcing. In section 3, we describe the model. In section 4, we present our analysis and discuss firms' sourcing decisions. In section 5, we provide the analysis of sequential mode of entry. Finally, we discuss the implications of our results and provide directions for further research in section 6.

2. Literature Review

The literature on outsourcing traditional IT functions is extensive, but the literature specifically on IT security outsourcing is limited. Dibbern et al. (2004) provides a comprehensive review of the IT outsourcing literature. Prior work has utilized transactional cost theory, agency theory, core-competency argument, and vendor-client relationship management to understand and explain why firms outsource IT, the benefits and risks associated with IT outsourcing, the IT functions outsourced, and factors that affect IT outsourcing outcomes. The bulk of this work relied on data collected through surveys.

Early research focused on cost savings as the primary motivation for outsourcing. Loh and Venkatraman (1992a) found that the degree of IT outsourcing was positively related to business and IT cost structures and negatively related to IT performance. On the other hand, McLellan et al. (1995) did not find any evidence for the hypothesis that firms with weak financial performance were more likely to outsource. Ang and Straub (1998) and Sobol and Apte (1995) concluded that firm size was negatively associated with the degree of outsourcing. Caldwell (2002) reported that one third of outsourcing contracts targeted at cost reductions failed to match the expectations.

Another stream of research explored the diffusion of IT outsourcing. Loh and Venkatraman (1992b) investigated whether the source of the influence of diffusion was internal (imitative behavior), external (external channels of communication such as media, etc.) or mixed (both). They concluded that the internal influence model explained the diffusion of IT outsourcing deals better than other models and that the internal influence was stronger after the Kodak's well-publicized outsourcing announcement. Reexamining the study by Loh and Venkatraman (1992b) with expanded data set, Hu et al. (1997) found that mixed influence was the dominant factor, and did not find support for the Kodak effect Ang and Cummings (1997) found that when the source of influence was federal regulators, banks responded more to institutional demands and less to strategic economic contingencies, and when the source of influence was peers, banks responded more to strategic economic contingencies. Slaughter and Ang (1996) found that firms were more likely to outsource jobs having volatile demand and requiring scarce skills. They explained their results using economies of scale and mitigation of technological risk arguments. DiRomualdo and Gurbaxani (1998) found that three strategic intents of IS outsourcing- IS improvement, business impact and commercial exploitation - impacted the degree of outsourcing and type of sourcing relationship.

Although IT security outsourcing is a widely discussed topic among the practitioner community, academic literature in IT security outsourcing is limited. Rowe (2007) suggested firms may enjoy benefits from network effects when they outsource IT security to the same MSSP. He argued that when more firms outsource to the same MSSP, the MSSP will be able to provide a better service to all customers because of access to a larger set of data and being able to analyze more network configurations. However, the MSSP could also become a more valuable target to attackers, increasing the likelihood of attack.

Very few papers in the information systems literature have developed economic models to understand either traditional IT or IT security outsourcing. Whang (1992) analyzed a multi-period software development contract between a firm and an outside developer and derived an optimal contact which replicates the equilibrium outcome of a benchmark in-house development. More recently, Sen at al. (2009) analyzed the impact of demand heterogeneity and variance in user preferences on the pricing and the allocation of resources for service-oriented models of information technology. Dey et al. (2008) analyzed different types of software outsourcing contracts under information asymmetry and incentive divergence and showed that by improvements on outsourcing process and control mechanisms, contract performance could be improved. In the IT security context, Ding et al. (2005) examined the characteristics of optimal MSSP contracts under moral hazard and reputation effects and found that an optimal contract should be performance based even in the existence of a strong reputation effect. In a subsequent work, Ding et al. (2006) showed that outsourcing decision is relatively insensitive to variation in service quality but highly sensitive to bankruptcy risk. Ding et al (2005b) showed that when transaction cost uncertainty or transaction costs are high, MSSPs are forced to charge a lower price to balance these costs. Gupta and Zhdanov (2007) analyzed the growth of MSSP network under a for-profit MSSP monopoly and under a consortium-based market structure.

The other literature on outsourcing has been in the manufacturing/production area and has primarily focused on principal-agent models to identify the conditions under which firms prefer outsourcing (Chalos and Sung 1998), the type of job that will be outsourced (Sridhar et al. 1997), and investment levels (Van Mieghem 1999).

The economic models considered in prior work on outsourcing typically relied on a principal-agent model with a single principal (the firm) and a single agent (the MSSP). However, our model incorporates the competition between two firms. Therefore, we are able to identify how competitive externalities influence firms' IT security outsourcing decisions.

3. Model Description

We consider an industry that has two competing firms, labeled as firm 1 and firm 2. Each firm offers a single product or service. The demand for the product of a firm is affected by whether one or both firms suffer from a security breach, in addition to its and the competing product's prices. The likelihood of a security breach on one or both firms depends on whether they manage their security in-house or they outsource their security. The specific assumptions of our model along with their justifications follow:

Assumption 1: The demand for the product of firm *i* is given by the following.

$$q_i = a - b_1 p_i + b_2 p_j + B_i \quad i, j \in \{1,2\}, i \neq j \tag{3.1}$$

where $a, b_1, b_2 > 0$ and $b_2 < b_1$. The linear competitive demand model given by (1) is standard in the literature (McGuire and Staelin 1983, Gal-Or and Ghose 2005). In (1), *a* represents the base demand to a firm when both firms set prices to zero and there is no security breach, b_1 denotes a firm's own price effect, b_2 denotes the cross-price effect, and B_i captures the change in firm *i*'s demand when firm *i*, firm *j*, or both *i* and *j* are breached.

Assumption 2:

$$\begin{aligned} &B_i = -\Delta, B_j = \alpha\Delta, \text{ if } i \text{ is breached and } j \text{ is not breached} \\ &B_i = -\Delta, B_j = -\Delta, \text{ if both } i \text{ and } j \text{ are breached} \\ &B_i = B_j = 0, \text{ if neither firm is breached} \end{aligned} \tag{3.2}$$

If firm *i* is breached and firm *j* is not, firm *i*'s demand decreases by Δ and firm *j* gets a fraction $\alpha \leq 1$ of Δ, and therefore, firm *j*'s demand increases by $\alpha\Delta$, and the industry's demand decreases by (1- α)Δ. Parameter α can be interpreted as a measure of the *degree of spillover* of demand to the non-breached competitor. The degree of spillover is likely to be dependent on factors such as the type (essential vs. non-essential) of product or service provided by the firms, substitutability of the products or services, and switching costs. For example, a publicized breach event in banking, health or pharmaceutical industry may cause more switching than a breach event in the manufacturing industry. When both firms are breached, each firm's demand decreases by Δ, resulting in a total decrease of 2Δ for the industry. The value of Δ is likely to be affected by factors related to the nature of breach, such as the sensitivity of customer information compromised in the breach as well as the product type. We assume that the decrease in demand due to a breach can not be larger than the primary demand each firm faces, i.e., $\Delta \leq a$.

Assumption 3: Firms can manage security through in-house operations or by outsourcing it to a MSSP. There is a single MSSP. While the assumption of single MSSP is not critical to our analysis[2], consolidation trends in MSSP industry and comments by security experts (Gartner 2005, Andrew Conry-Murray 2006, Berthillier 2005) suggest that MSSP industry is likely to have few large players.

[2] We discuss the impact of relaxing the single MSSP assumption in Section 6.

Assumption 4: The joint probability distribution for the breach events at the two firms when firm 1 decides X and firm 2 decides Y, $X, Y \in \{outsource(O), in-house(I)\}$, is given by the following probability matrix.

		Firm 2	
		Breached	Non-Breached
Firm 1	Breached	P^{XY}	$\theta^X - P^{XY}$
	Non-Breached	$\theta^Y - P^{XY}$	$1-\theta^X - \theta^Y + P^{XY}$

Table 1. Joint Probability Distribution of Breach Events

The marginal probability of a security breach for a firm when it outsources and when it manages in-house is θ^{O} and θ^{I}, respectively. A lower marginal probability implies a higher level of protection or a higher quality of security services. The quality of security services is likely to depend on the technology and expertise used by the firm managing the security services. We denote the environment in which $\theta^O < \theta^I$ as the *High Quality Outsourcing* environment, and that in which $\theta^O > \theta^I$ as the *Low Quality Outsourcing* environment.

The probability that both firms are breached is P^{XY}. A higher value for P^{XY} implies that the breach events in the two firms are more correlated. Whether the degree of correlation will be higher when both firms outsource than when one or both firms do not outsource will depend critically on the function outsourced. If the MSSP specializes in the management of security infrastructure that includes firewall, IDS, and other security technologies, then the MSSP is likely to use same or similar technologies and expertise to manage the security of both firms in order to take advantage of economies of scale. In this case, the correlation between breach events in two firms is likely to be higher when both firms outsource than when one or both do not, i.e., $P^{OO} > P^{OI}, P^{II}$. If the MSSP specializes in monitoring services, then it is likely to focus on observing and analyzing the breach event on firms and use information pertaining to breach on one firm and protect the other firm from a similar breach, if it is not already breached. That is, MSSP facilitates information-sharing relationship between firms (Rowe 2007). In this case, the joint probability of breach in two firms is likely to be lower when both firms outsource than either one or both do not, i.e., $P^{OO} < P^{OI}, P^{II}$. In the light of above arguments, we characterize an MSSP environment as belonging to one of the four regions given in Figure 1. The vertical axis denotes the difference in the quality of MSSP and that of in-house management, $\theta^O - \theta^I$. The horizontal axis denotes the difference in the joint probability of breach events in two firms when both firms outsource IT security and that when only one firm outsources IT security.

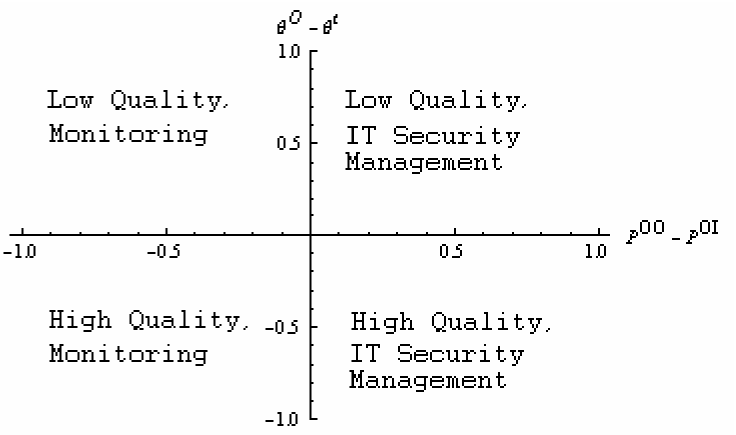

Figure 1. MSSP operating regions

Assumption 5. The firms have a fixed budget for managing information security, and they spend this budget on security whether they outsource or manage in-house. This assumption is consistent with current industry practices in information security. Further, we assume that the budget is the same and is normalized to zero in order to eliminate the impact of cost differences in firm's outsourcing decisions[3] and to focus on the impact of competition, industry, and breach characteristics.

Assumption 6. The marginal cost of production is fixed and is normalized to zero. This assumption does not affect the results qualitatively.

Assumption 7. We consider a one shot, 3-stage non-cooperative game. The sequence of events is the following. In stage 1, each firm decides whether to outsource security or manage it in-house. In stage 2,

[3] Note that for the same budget, MSSP could offer a higher (or a lower) quality than in-house operations. So, θ^O and θ^I could be viewed as cost-adjusted quality measures.

nature moves and the breach events occur. After observing breach events at stage 2, firms set their prices simultaneously at stage 3. The assumption that outsourcing decisions are made before price decisions indicates that outsourcing decisions are more strategic and long-term compared to price decisions for firms. This is consistent with the empirical observation that IT outsourcing contracts tend to be long-term (Gurbaxani 2006). The assumption also indicates that price decisions are flexible in the sense that prices can be changed relatively easily and frequently.

Assumption 8. All model parameters are common knowledge. This assumption allows us to analyze the strategic interaction between firms caused by competition, MSSP, and breach characteristics, which is the focus of this paper.

4. Model Analysis

We use backward induction to solve for the Nash equilibrium for the sourcing game. At stage three, after observing the breach events (if any), both firms choose their prices simultaneously by maximizing their individual payoffs. The payoff for firm i , π_i , is given by the following.

$$\pi_i = p_i q_i = p_i (a - b_1 p_i + b_2 p_j + B_i) \tag{4.1}$$

Solving simultaneously the first-order conditions for the maximization problems of both firms, we obtain the following optimal price for firm *i* in stage 3 of the game. Details of this and other derivations as well as proofs of propositions in this paper are provided in the Appendix.

$$p_i^* = \frac{a(2b_1 + b_2) + 2b_1 B_i + b_2 B_j}{4b_1^2 - b_2^2} \tag{4.2}$$

The values for B_i and B_j depend on the breach scenario (viz., zero, one, or two breached firms) is realized in stage 2. Substituting (3.2) in (4.2), we obtain the following optimal prices in stage 3.

$$p_i^* = \begin{cases} \dfrac{a}{2b_1 - b_2} \text{ if neither firm is breached} \\ \\ \dfrac{2b_1(a+\alpha\Delta)+b_2(a-\Delta)}{4b_1^2 - b_2^2} \text{ if firm } i \text{ is not breached and firm } j \text{ is breached} \\ \dfrac{2b_1(a-\Delta)+b_2(a+\alpha\Delta)}{4b_1^2 - b_2^2} \text{if firm } i \text{ is breached and firm } j \text{ is not breached} \\ \dfrac{a-\Delta}{2b_1 - b_2} \text{ if both firms are breached} \end{cases} \qquad (4.3)$$

We make the following observations regarding the optimal prices in stage 3. The price charged by the breached firm is lower than that charged by firms when there is no breach and that charged by the non-breached firm, but is higher than that charged when both firms are breached. These observations are intuitive and can be explained by the demand effects of the breach events. We also observe that the non-breached firm's price (when its competitor is breached) may be higher or lower than the price charged when there are no breaches; it is higher when $\alpha > \dfrac{b_2}{2b_1}$ and is lower otherwise. This shows that if the spill-over demand, relative to the degree of price competition, is not sufficiently large, then the non-breached firm is unable to take advantage of the increase in its demand and charge a higher price because, at high levels of price competition, the non-breached firm is forced to reduce its price in response to the lower price charged by the breached firm.

Substituting (4.3) in (4.1), we find that $\pi_i = b_1\left(p_i\right)^2$ under any breach scenario. Therefore, the breached firm always sees a reduction in its profit. However, the non-breached firm may see its profit increase or decrease depending on whether $\alpha > \dfrac{b_2}{2b_1}$. Breach has a direct effect and an indirect effect on the non-breached firm. The direct effect is that it enjoys a higher primary demand, ceteris paribus, because of the spillover of consumers from the breached firm. The indirect effect is that the changes in demands of the two firms force the firms to change their prices, which may or may not favor the non-breached firm. Depending on which effect dominates, a non-breached firm may be rewarded or penalized by a breach on the competitor.

In stage 1 of the game, each firm simultaneously makes its sourcing decision by maximizing its expected payoff in stage 3 of the game. The expected payoff for a firm depends on the outsourcing decisions of both firms. The expected payoff for firm *i* in stage 1, $E\pi_i$, is given by the following.

$$E\pi_i=\begin{cases}
b_1\left(\begin{aligned}&P^{OO}\left(\frac{a-\Delta}{2b_1-b_2}\right)^2+(1-2\theta^O+P^{OO})\left(\frac{a}{2b_1-b_2}\right)^2+\\&(\theta^O-P^{OO})\left(\left(\frac{2b_1(a+\alpha\Delta)+b_2(a-\Delta)}{4b_1^2-b_2^2}\right)^2+\left(\frac{2b_1(a-\Delta)+b_2(a+\alpha\Delta)}{4b_1^2-b_2^2}\right)^2\right)\end{aligned}\right) & \text{if both outsource}\\
b_1\left(\begin{aligned}&P^{OI}\left(\frac{a-\Delta}{2b_1-b_2}\right)^2+(\theta^O-P^{OI})\left(\frac{2b_1(a-\Delta)+b_2(a+\alpha\Delta)}{4b_1^2-b_2^2}\right)^2+\\&(\theta^I-P^{OI})\left(\frac{2b_1(a+\alpha\Delta)+b_2(a-\Delta)}{4b_1^2-b_2^2}\right)^2+(1-\theta^O-\theta^I+P^{OI})\left(\frac{a}{2b_1-b_2}\right)^2\end{aligned}\right) & \text{if } i \text{ outsources and } j \text{ does not}\\
b_1\left(\begin{aligned}&P^{OI}\left(\frac{a-\Delta}{2b_1-b_2}\right)^2+(\theta^I-P^{OI})\left(\frac{2b_1(a-\Delta)+b_2(a+\alpha\Delta)}{4b_1^2-b_2^2}\right)^2+\\&(\theta^O-P^{OI})\left(\frac{2b_1(a+\alpha\Delta)+b_2(a-\Delta)}{4b_1^2-b_2^2}\right)^2+(1-\theta^O-\theta^I+P^{OI})\left(\frac{a}{2b_1-b_2}\right)^2\end{aligned}\right) & \text{if } j \text{ outsources and } i \text{ does not}\\
b_1\left(\begin{aligned}&P^{II}\left(\frac{a-\Delta}{2b_1-b_2}\right)^2+(\theta^I-P^{II})\left(\left(\frac{2b_1(a+\alpha\Delta)+b_2(a-\Delta)}{4b_1^2-b_2^2}\right)^2+\left(\frac{2b_1(a-\Delta)+b_2(a+\alpha\Delta)}{4b_1^2-b_2^2}\right)^2\right)+\\&+(1-2\theta^I+P^{II})\left(\frac{a}{2b_1-b_2}\right)^2\end{aligned}\right) & \text{if neither outsources}
\end{cases}\tag{4.4}$$

We define the following variables for ease of exposition.

$$L=\frac{\Delta b_1(2b_1-\alpha b_2)((4a-2\Delta)b_1+(2a+\alpha\Delta)b_2)}{(4b_1^2-b_2^2)^2}\tag{4.5}$$

$$V=\frac{\Delta b_1(2\alpha b_1-b_2)(2(2a+\alpha\Delta)b_1+(2a-\Delta)b_2)}{(4b_1^2-b_2^2)^2}\tag{4.6}$$

$$L^{'}=\frac{\Delta b_1(2a-\Delta)}{(2b_1-b_2)^2}\tag{4.7}$$

We can show that L and V, respectively denote the decrease in profit to the breached firm and the increase in profit to the non-breached firm when only one firm is breached, and $L^{'}$ denotes the loss of profit to each firm when both firms are breached. Note that L and L' are always positive, but V is positive when $\alpha > \frac{b_2}{2b_1}$ and negative when $\alpha < \frac{b_2}{2b_1}$. (4.4) can now be written using the payoff matrix shown in Figure 2. The first (second) element in the ordered pair within each cell is the expected payoff to firm 1 (firm 2).

Firm 2

		O	***I***
Firm 1	***O***	$\left(\begin{array}{l} -P^{OO}L^{'} + (\theta^{O} - P^{OO})(V-L), \\ -P^{OO}L^{'} + (\theta^{O} - P^{OO})(V-L) \end{array}\right)$	$\left(\begin{array}{l} -P^{OI}L^{'} + (\theta^{I} - P^{OI})V - (\theta^{O} - P^{OI})L, \\ -P^{OI}L^{'} + (\theta^{O} - P^{OI})V - (\theta^{I} - P^{OI})L \end{array}\right)$
	I	$\left(\begin{array}{l} -P^{OI}L^{'} + (\theta^{O} - P^{OI})V - (\theta^{I} - P^{OI})L, \\ -P^{OI}L^{'} + (\theta^{I} - P^{OI})V - (\theta^{O} - P^{OI})L \end{array}\right)$	$\left(\begin{array}{l} -P^{II}L^{'} + (\theta^{I} - P^{II})(V-L), \\ -P^{II}L^{'} + (\theta^{I} - P^{II})(V-L) \end{array}\right)$

Figure 2. Normal Form of the game in Stage 1

We define the variable $R = \left(\frac{V + L^{'}}{L}\right)$ which replaces all cost and benefit terms in the above figure and allows us to analyze the total impact of these terms using a single variable. The numerator denotes, given that the competitor is breached, how much higher the firm's profit is if it is not breached than if it is breached. Similarly, the denominator shows the same profit difference given that the competitor is not breached. This is a ratio of the (net) value a firm obtains from being non-breached when the competitor is breached to that when the competitor is not breached, i.e., a measure of the relative value non-breached firm gets from the competitor's breach. Note that R can be less than 1 or greater than 1. R describes, in a restrictive sense, the competitive risk associated with security breaches. That is, it measures the relative benefit to loss a firm realizes if only one of the two competing firms is breached. Note that if both firms are breached or no firm is breached, neither firm has a competitive advantage over the other. If R >1, then a firm realizes a positive expected payoff given that only one firm is breached. Following the terminology used in (Tarantino 2008), we label this environment as "speculative risk" environment. We label the environment in which R <1 as “non-speculative risk” environment, and in this case, a firm realizes a negative expected payoff given only one firm is breached.

The following result characterizes the Nash equilibrium outcome for the sourcing game.

Lemma 1: *The Nash equilibrium outcome for the sourcing game is given by the following:*

$$\begin{cases} \textit{(outsource,outsource),if } \left(\theta^{O}-\theta^{I}\right)<(P^{OI}-P^{OO})(R-1) \\ \textit{(In-house,In-house),if } \left(\theta^{O}-\theta^{I}\right)>Max\left((R-1)(P^{II}-P^{OI}),(R-1)(P^{OI}-P^{OO})\right) \\ \textit{Mixed strategy with probability of outsourcing} \dfrac{(P^{II}-P^{OI})(R-1)-\left(\theta^{O}-\theta^{I}\right)}{(2P^{OI}-P^{OO}-P^{II})(R-1)}, \textit{ otherwise} \end{cases}$$

Lemma 1 shows that a firm’s outsourcing decision depends critically on three factors: the quality of the MSSP relative to that of in-house security management, the security function (viz., security monitoring or infrastructure management) outsourced, and the ratio R. Figure 3 illustrates the regions where the different decisions are optimal for the firms for a speculative risk environment. In the region below line AB, both firms outsource. In the shaded region above line AB, both firms manage in house, and in the non-shaded region, each firm outsources with a probability as given in Lemma 1. It is evident from the figure that even when the MSSP does not offer a higher quality than in-house management, both firms may outsource (see the shaded region below line AB in quadrant II).

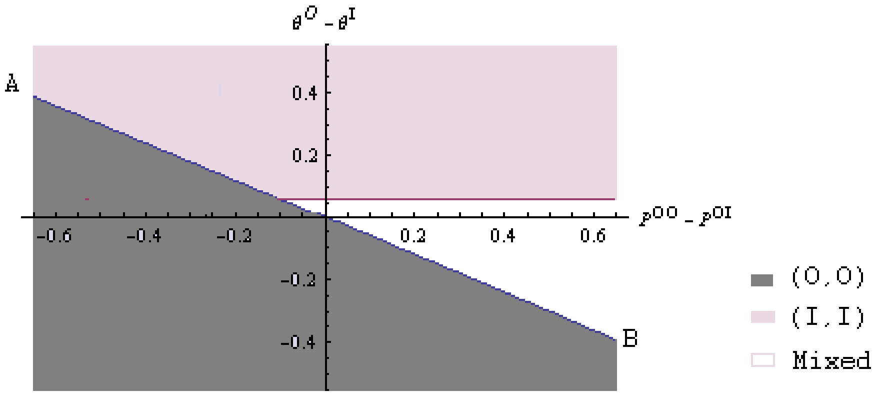

Figure 3. Sourcing regions for $P^{OI}=0.35, P^{II}=0.45, R=1.6$

Because our interest is in deriving insights about how the risk environment, the MSSP, industry and breach characteristics affect the firms' outsourcing decisions, we next analyze each of these impacts separately.

4.1. Impact of Competitive Risk Environment on Firm's Outsourcing Decisions

We show the following result.

Proposition 1: *(a) If R=1, then both firms outsource iff the MSSP provides a higher quality than in-house management and both firms manage in-house otherwise.* (*b) An increase in R leads to an increase in the likelihood of both firms outsourcing if security monitoring is outsourced and a decrease in the likelihood of both firms outsourcing if security infrastructure management is outsourced.*

Proposition 1 provides important insight into the role played by the risk environment in firms' decisions to outsource security. The environment is speculation-risk-neutral (i.e., $R = 1$) when either the firms are not competitors or firms do not expect a net benefit from the competitor's breach. In this environment, firms will outsource security if and only if the MSSP offers a quality advantage over in-house management. It is worthwhile to note that security researchers and practitioners frequently cite quality or cost advantages of MSSPs as the primary reason for firms to outsource security (Wylder 2004, pp 199-200). While this conventional explanation is consistent with our result, it is only partial. Specifically, the explanation based solely on quality or cost advantage does not provide any insights into the role of strategic factors or the security function outsourced on the firms' decisions.

We find that when firms do compete with each other, based on either price or breach events, strategic considerations, in particular the nature and extent of risk, influence firms' decisions. When firms face speculative or non-speculative risk from security breaches, they may outsource even when the MSSP does not offer a quality advantage. For example, as it is seen in Figure 3, even when $\theta^O > \theta^I$, both firms outsource monitoring function in the shaded region below line AB in quadrant II. Furthermore, Proposition 1 shows that the security function also plays an important role in firms' outsourcing decisions. For instance, if the MSSP does not offer a higher overall quality than in-house management, then both firms will likely manage security infrastructure management in house.

Proposition 1.b shows the impact of extent of competitive risk on firms' decisions and is illustrated visually using Figure 4a and Figure 4b. An increase in *R*, shown by the clockwise movement of the line AB, increases the likelihood of outsourcing the security monitoring function by both firms and decreases the likelihood of outsourcing infrastructure management by both firms. *R* is higher when the expected payoff to a firm given that one is breached and the other is not breached is higher, which implies that a scenario in which one is breached and the other is not becomes more profitable to a firm at higher values of *R*. Therefore, the outsourcing decision that increases the likelihood of this scenario becomes more attractive to firms. Because outsourcing security monitoring increases the likelihood of only one firm being breached, firms have more incentives to outsource security monitoring. Using the same logic, we can explain why firms are less likely to outsource infrastructure management when *R* increases. In essence, as the risk associated with the security environment becomes more speculative, firms are more (less) likely to outsource monitoring (infrastructure management).

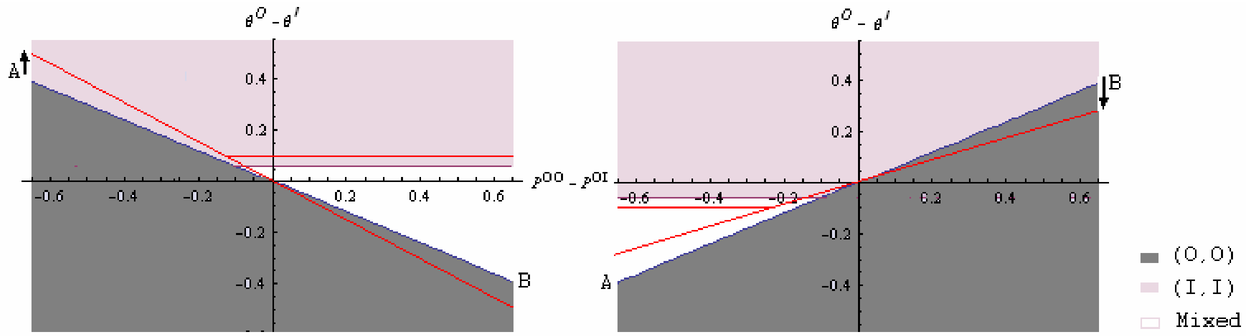

Figure 4a. Impact of Reward-to-risk ratio for $P^{OI} = 0.35, P^{II} = 0.45, R = 1.6$

Figure 4b. Impact of Reward-to-risk ratio for $P^{OI} = 0.35, P^{II} = 0.45, R = 0.4$

4.2. Impact of MSSP Characteristics on Firms' Outsourcing Decisions

In our model, the MSSP is characterized by two parameters: the marginal probability of breach for the outsourcing firm (θ^O), which measures the overall quality of service offered by the MSSP and the joint probability of breach events in the two firms (p^{OO}), which measures, in some sense, the relative degree of security monitoring vis-à-vis infrastructure management services offered by the MSSP. A higher value for p^{OO} often suggests that the MSSP focuses more on infrastructure management and less on security monitoring.

We show the following result.

Proposition 2: *(a) An improvement in the MSSP quality leads to more outsourcing by both firms irrespective of the security function outsourced. (b) an increase in* p^{OO} *decreases the likelihood of both firms' outsourcing if R>1, and increases the likelihood of both firms' outsourcing, otherwise.*

Proposition 2(a) is intuitive because an improvement in MSSP quality improves a firm's payoff from outsourcing. Further, if the firms compete with each other, then an improvement in the MSSP quality hurts the payoff of the firm that manages security in-house. Therefore, both firms have a higher incentive to use the MSSP, and firms that manage security in-house may shift to the outsourcing strategy if the MSSP quality increases. In figure 3, an improvement in the MSSP quality can be shown as a downward movement on the vertical axis, which represents a movement towards the outsourcing region.

Figure 5a and Figure 5b illustrate Proposition 2(b). An increase in p^{OO} is shown as a horizontal movement to the right, from the initial position at $(x_{1,}\ y_1)$ to the final position at $(x_2,\ y_1)$ after the increase in p^{OO}. In Figure 5a, in which *R*>1, $(x_{1,}\ y_1)$ lies in the region where both firms outsource and $(x_2,\ y_1)$ lies in the region where both firms manage in-house. We find the opposite in Figure 5b, in which *R*<1.

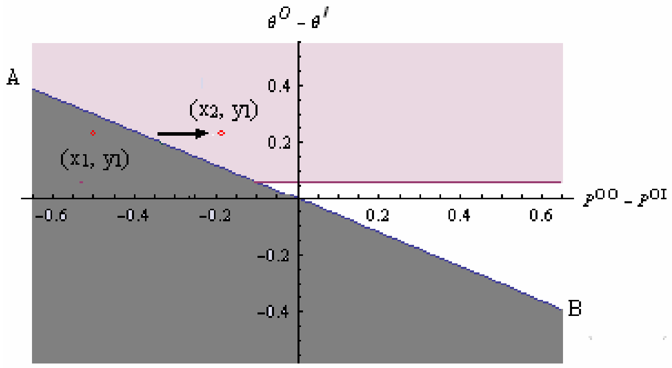

Figure 5a. Impact of MSSP Specialization for $P^{OI} = 0.35, P^{II} = 0.45, R = 1.6$

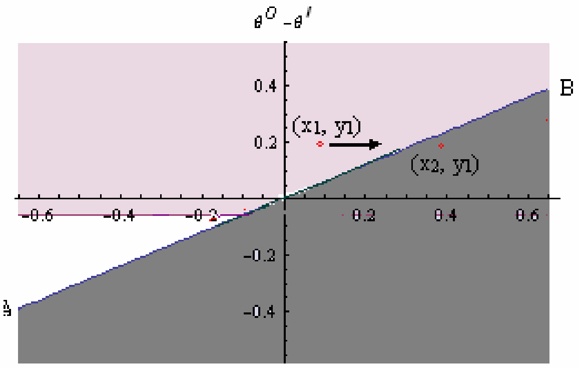

Figure 5b. Impact of MSSP Specialization for $P^{OI} = 0.35, P^{II} = 0.45, R = 0.4$

The intuition underlying Proposition 2(b) can be explained as follows. When *R*>1, the positive expected benefit in the scenario in which only one firm is breached induces firms to prefer an environment in which only one of them is breached to that in which both firms are breached. Therefore, if the joint probability of breach increases, then firms' incentives to outsource decreases. When *R*<1, the expected benefit in the scenario in which only one firm is breached is negative. So, firms prefer an environment in which both are breached to the environment in which only one of them is breached. Thus, in this case, an increase in the joint probability of breach events in two firms increases both firms' incentives to outsource.

It is worthwhile to compare Proposition 2 with prior results about firms' reluctance to share security information Prior research showed that positive externality effects of information sharing may discourage firms to share security information with one another (Gordon et al. 2003). Leakage of sensitive information has also been cited as a reason for firms' reluctance to share security information (Gal-Or and Ghose 2005) which may lead to the loss of the market value of the firm due to negative publicity (Cavusoglu et al. 2004). Though we do not model information sharing explicitly, security experts have argued that security monitoring of two firms by the same MSSP is an indirect way of sharing breach information through an intermediary (Rowe 2007), and it is the information that the MSSP obtains by analyzing the breach on one firm that enables the MSSP to prevent a breach on the other firm, and thereby reducing the probability of both firms being breached. In sharp contrast to prior results, we find that firms may have a greater incentive to share security information by outsourcing the monitoring function if the MSSP can use that information to decrease the joint probability of breaches more. This result holds in the speculative risk environment because, as we stated earlier, firms prefer an environment in which only one of them is breached to that in which both firms are breached in this environment. The difference between our results and that of prior research can be attributed to the observation that prior research considered the improvements in the efficiency of security investments in terms of a reduction in the breach probability enabled by information sharing whereas we consider the use of information to reduce the joint probability of breaches.

4.3. Impact of Breach Characteristics on Firms' Outsourcing Decisions

The parameters that characterize a breach in our model are the extent of spillover α, and the breach severity Δ. We note from (4.5) – (4.7) and from Lemma 1 that the breach parameters affect firms' decisions only through their impact on the value of R. Therefore, the security risk environment is determined partly by breach characteristics[4], and once the impact of these parameters on the risk environment is known, the impact on firms' decisions can be determined using Proposition 1(b). We have the following result regarding the impact of breach characteristics on firms' outsourcing decisions.

Proposition 3: *(a) An increase in spillover increases the likelihood of both firms' outsourcing security monitoring and decreases the likelihood of both firms' outsourcing infrastructure management.*

(b) An increase in breach severity increases the likelihood of both firms' outsourcing security monitoring and decreases the likelihood of both firms' outsourcing infrastructure management if $\alpha > \frac{2b_2}{2b_1 - b_2}$ *and decreases the likelihood of both firms' outsourcing security monitoring and increases the likelihood of both firms' outsourcing infrastructure, otherwise.*

Proposition 3(a) is a surprising result because one would expect that when the competition induced by spillover effects of security breaches becomes more intense, firms will prefer an environment in which the likelihood of only one firm being breached is smaller to one in which this likelihood is larger so as to mitigate the spillover effect. However, Proposition 3(a) implies the opposite. The reason for the counter-intuitive result can be attributed to the following. Using (4.3), we find that the price charged by the non-breached firm as well as by the breached firm increases in spillover (α). Therefore, the loss to breached firm (L) decreases in spillover and the benefit to non-breached firm (V) increases in spillover[5]. Since there is no switching when both firms are breached, α has no impact on $L^{'}$. Hence, an increase in the demand spillover caused by security breaches makes the risk environment more speculative, which favors outsourcing of security monitoring.

The impact of breach severity on the risk environment can also be explained using how an increase in Δ affects the reward and risk from a security breach. Consider the scenario in which one firm is breached. A larger value for Δ implies that the breached firm will face a larger reduction in demand and therefore a larger reduction in profit if it is breached. Therefore, the risk from getting breached is

[4] Other demand parameters such as a, b_1, and b_2, also affect the risk environment.

[5] Note that a firm's profit is directly proportional to the square of price it charges.

higher when Δ is larger. Now consider the scenario in which no firm is breached. If the competitor is breached, then the demand to a non-breached firm is higher when Δ is larger. However, the marginal increase in demand to a non-breached firm is smaller than the marginal decrease in the demand for the breached firm. In this scenario, the breached firm will set its price more aggressively, causing an even smaller increase in the reward to the non-breached firm. In order to make the risk environment more speculative (i.e., increase *R*) when Δ increases, the spillover rate has to be sufficiently large so that the increase in reward because of the competitor breach offsets the increase in risk.

In summary, our analysis shows that firms have stronger incentives to outsource security if the MSSP offers a higher quality in terms of preventing breaches compared to in-house management. However, a higher quality is neither a prerequisite nor a guarantee for a firm to outsource security. The competitive risk environment and the nature of the security function outsourced, in addition to quality, determine firms' outsourcing decisions. If the reward from the competitor's breach is higher than the loss from own breach, then even if the likelihood of a breach is higher under the MSSP, the expected benefit from the competitive demand externality may offset the loss from the higher likelihood of breaches, resulting in one or both firms outsourcing security. The incentive to outsource security monitoring is higher than that of infrastructure management because the MSSP can reduce the likelihood of breach on both firms and thus enhance the demand externality effect. The incentive to outsource security monitoring (infrastructure management) is higher (lower) if either the likelihood of breach on both firms is lower (higher) when security is outsourced or the benefit (relative to loss) from the externality is higher (lower). The benefit from the demand externality arising out of a security breach is higher when more of the customers that leave the breached firm switch to the non-breached firm.

5. Sequential Entry

In the previous section, we assumed that firms make their outsourcing decisions simultaneously. In the traditional IT outsourcing market, numerous examples of firms following the outsourcing strategy of other firms have been observed, a phenomenon referred to as the "Kodak effect" in the IT community (Loh and Venkatraman 1992). While the IT security outsourcing market is still in its early stages to offer evidence of a similar phenomenon, it is conceivable that some firms may wait to make their own decisions until other, perhaps major, players outsource their security functions. We analyze in this section the incentives of firms to be the leader or the follower in outsourcing IT security. The model parameters and assumptions, except the one related to stage 1 of the game stated in assumption 7, remain the same. In stage 1 of the game, we assume, without loss of generality, that firm *i* first decides whether to outsource security followed by firm *j*. We further assume that the outsourcing decision, once made, cannot be changed afterward. We have the following result that characterizes the equilibrium in the sequential game.

Lemma 2: *The Nash equilibrium outcome for the sequential sourcing game is given by the following:*

$$\begin{cases} \textit{(outsource, outsource), if } \left(\theta^{O}-\theta^{I}\right)<(P^{OI}-P^{OO})(R-1) \\ \textit{(in-house, in-house), if } \left(\theta^{O}-\theta^{I}\right)>Max\left((R-1)(P^{II}-P^{OI}),(R-1)(P^{OI}-P^{OO})\right) \\ \textit{(outsource, in-house), if } (P^{OI}-P^{OO})(R-1)<\left(\theta^{O}-\theta^{I}\right)<(P^{II}-P^{OI})(R-1) \textit{ and } \theta^{O}<\theta^{I} \\ \textit{(in-house, outsource), if } (P^{OI}-P^{OO})(R-1)<\left(\theta^{O}-\theta^{I}\right)<(P^{II}-P^{OI})(R-1) \textit{ and } \theta^{O}>\theta^{I} \end{cases}$$

where the first strategy within the parenthesis denotes the leader's choice and the second one denotes the follower's response.

Comparing Lemma 1 and Lemma 2, we find that the equilibria in the simultaneous and sequential games are identical except the mixed strategy region in the simultaneous game is replaced with the following two pure strategy equilibria in the sequential game: i) the leader chooses outsourcing IT security and the follower chooses in-house management, and ii) the leader chooses in-house management and the follower chooses outsourcing. That is, the region in which both firms outsource and the region in which both firms manage in house are identical in the simultaneous and sequential games.

It is easy to show that when the firms make different decisions, the payoff to the leader is higher than to the follower because of the first-mover advantage enjoyed by the firm. Lemma 2 shows that if the firms make different decisions, then the leader always chooses the option that offers a higher quality and forces the follower to choose the lower quality option, irrespective of other parameter values. Therefore, while risk environment and the type of function outsourced determine whether both firms outsource or both firms manage in house, they do not affect the decisions of the leader and the follower when only one firm outsources.

In the rest of this section, we focus on the asymmetric equilibrium in our discussion related to the impact of risk environment, MSSP characteristics, and breach characteristics on the firms' strategies

***Proposition 4*:**

If an asymmetric equilibrium (either (outsource, in-house) or (in-house, outsource)) is played in the sequential game, then an increase in R decreases the likelihood of that equilibrium when R<1 and increases the likelihood of that equilibrium when R>1, irrespective of the function outsourced.

Proposition 4 implies that the incentives of the leader and those of the follower to stick to their strategies are enhanced when *R* increases in a speculative risk environment. The intuition for this result is as follows. In a speculative risk environment, assuming an asymmetric equilibrium, the leader will outsource infrastructure management and the follower will manage in-house if the quality of the MSSP is higher, but not very much higher, than that of in-house management. In this case, if the leader chooses outsourcing, then the follower chooses in-house management because the high correlation of breach events when it also chooses outsourcing reduces the benefit from the competitive externality imposed by a breach. Further, the relatively low quality advantage offered by the MSSP does not offset the loss in the benefit from competitive externality in this case. Anticipating the follower's incentive to manage in-house, the leader chooses outsourcing to take advantage of the higher quality and a smaller breach probability. When the benefit from competitive externality (or *R*) is higher, the follower's incentives to choose in-house management when the leader chooses outsourcing, and the leader's incentives to exploit the MSSP's quality advantage are enhanced. Firms have the opposite incentives when *R*<1, and therefore, the impact of *R* on the firms' strategies is also reversed.

Proposition 5:

(a) If an asymmetric equilibrium (either (outsource, in-house) or (in-house, outsource)) is played in the sequential game, then an increase in the MSSP quality decreases the likelihood of that equilibrium, irrespective of the function outsourced.

(b) If an asymmetric equilibrium (either (outsource, in-house) or (in-house, outsource)) is played in the sequential game, then an increase in p^{OO} *decreases the likelihood of that equilibrium when R<1 and increases the likelihood of that equilibrium when R>1, irrespective of the function outsourced.*

Proposition 5(a) is intuitive because an increase in the MSSP quality always makes the outsourcing option more attractive, increasing the likelihood of both firms outsourcing. The reasoning for Proposition 5(b) is similar to that for Proposition 4. When *R>1,* the leader is the one that will outsource if MSSP has a quality advantage and it will outsource infrastructure management. An increase in p^{OO} decreases the follower's incentive to choose the outsourcing option in a speculative risk environment, causing the leader to choose MSSP for its quality advantage. The reverse happens when *R<1.*

As we explained in Section 4, breach characteristics affect firms' decisions indirectly by their impact on *R*. The impact of these characteristics on *R* is same whether the firms play a simultaneous or a sequential game, and proposition 4 illustrates the impact of *R* on the firms in a sequential game. Therefore, we simply state the result regarding the impact of breach characteristics in a sequential game as the following proposition without any discussion.

Proposition 6: *(a) If an asymmetric equilibrium (either (outsource, in-house) or (in-house, outsource)) is played in the sequential game, then an increase in spillover increases the likelihood of that equilibrium when R>1 and decreases the likelihood of that equilibrium when R<1, irrespective of the function outsourced.*

(b) If an asymmetric equilibrium (either (outsource, in-house) or (in-house, outsource)) is played in the sequential game, then an increase in breach severity increases the likelihood of that equilibrium when R>1 and $\alpha > \frac{2b_2}{2b_1 - b_2}$ *(or R<1 and* $\alpha < \frac{2b_2}{2b_1 - b_2}$*) and decreases the likelihood of that equilibrium when R>1 and* $\alpha < \frac{2b_2}{2b_1 - b_2}$ *or (or R<1 and* $\alpha > \frac{2b_2}{2b_1 - b_2}$*), irrespective of the function outsourced.*

6. Conclusion

The risks associated with IT security are fundamentally different from those associated with traditional IT functions. However, the reasons cited by both academics and security experts for why firms outsource IT security are the same as those cited for outsourcing of traditional IT functions. We believe that the IT security outsourcing decision is a strategic one in which a firm considers the ramifications of the competitor's action on its payoff and vice versa. Ignoring such strategic considerations and solely using criteria related to cost or quality measures in IT security outsourcing decision making process may result in sub-optimal decisions. To this end, while analyzing firms' decision to outsource IT security, we consider the information security risk not only as a form of non-speculative risk but also a form of speculative risk and analyze the impact of competitive externalities on firms' incentives to outsource IT security. Thus we offer a novel explanation for firms' decision to outsource IT security based on such externalities.

We show that a firm's outsourcing decision depends critically on the interaction of the quality of the MSSP relative to that of in-house security management, MSSP specialization, and the risk environment. Consistent with the traditional explanation given for firms' outsourcing decision, we also found that if outsourcing leads to a lower probability of breach, then firms outsource security if competition is not an issue. However, because of the competitive externalities, firms may prefer outsourcing even if it does not reduce the breach probability. Nevertheless, an improvement in MSSP quality leads to more outsourcing. If firms operate in a speculative risk environment, then they outsource more if MSSP is specialized in monitoring and less if MSSP is specialized in management of security infrastructure. However, when firms operate in a non-speculative risk environment, then they outsource more if MSSP is specialized in management of security infrastructure and less if MSSP is specialized in monitoring. The risk environment becomes more speculative with increases in spillover and in breach severity if spillover is higher than a threshold.

We made a number of simplifying assumptions to make the analysis tractable. However, the qualitative nature of or results will likely hold even when we relax many of these assumptions. We discuss the impact of relaxing some of the more critical assumptions in the following paragraphs. One, we assumed that there is a single MSSP. Existence of multiple MSSPs complicates the analysis in two ways. The MSSPs may specialize in different security functions, and the two firms may outsource to different MSSPs. If the MSSPs offer the same function, then the analysis for the cases in which neither firm outsources, only one of the firms outsources, and both firms outsource to the same MSSP remains the same as in this paper. Even when the firms outsource to different MSSPs, if the firms outsource infrastructure management and the MSSPs apply similar procedures and best practices, then our analysis and results will hold. On the other hand, if the firms outsource security monitoring, then it is likely that the probability of breach events is not likely to be as low as when there is a single MSSP unless the MSSPs share their information about breach events. The modeling and analysis of the case when the MSSPS offer different functions, and the firms outsource to different MSSPs is challenging and requires further research. Two, we assumed identical firms, ex ante. A model with heterogeneous firms will offer insights into how firm-specific factors such as firm size affect outsourcing decisions. Three, we assumed MSSP parameters and the firms' investment in security as exogenous. However, some of these parameters can be dependent on each other, and endogenizing these parameters could be possible extensions to the model.

References

Ang, S. and Cummings, L. L. (1997). "Strategic Response to Institutional Influences on Information Systems Outsourcing," Organization Science, Vol. 8, No. 3, pp. 235-256.

Ang, S. and Straub, D. W. (1998). "Production and Transaction Economies and IS Outsourcing: A Study of the U.S. Banking Industry," MIS Quarterly, Vol. 22, No. 4, pp. 535-552.

Bank for International Settlements, (June 2004), "Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework.", http://www.bis.org/publ/bcbs107.htm

Berthillier, A. (2005), "Managed Security Services for Network Service Provider, " Juniper Networks Inc. Solution Brief.

Caldwell, T ‘Downturn gives a lift to outsourcing’. IT services and solutions. Management consultants association, 2002, p.2.

Cavusoglu, H., Mishra, B., Raghunathan, S. (2004). “The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers**,”** International Journal of Electronic Commerce, Vol. 9, No. 1, pp. 70-104.

Chalos, P. and Sung, J. (1998). "Outsourcing Decisions and Managerial Incentives," Decision Sciences, Vol.29, No. 4, pp. 901-919.

Conry-Murray, A. (2006). "Bye-Bye Independent Managed Security Providers, " Network Computing, Vol. 17 No. 24. pp.18.

Dey, D., Fan, M., Zhang, C. (2008) "Design and Analysis of Contracts for Software Outsourcing, " Forthcoming in Information Systems Research

Dibbern, J., Goles, T., and Hirschheim, R (2004). "Information Systems Outsourcing: A Survey and Analysis of the Literature, " The DATA BASE for Advances in Information Systems, Vol. 35, No. 4.

Ding, W., W. Yurcik, and X. Yin (2005a). "Outsourcing Internet Security: Economic Analysis of Incentives for Managed Security Service Providers. " Workshop on Internet and Network Economics (WINE), Hong Kong, China, December 15-17.

Ding, W. and W. Yurcik (2005b). “Outsourcing Internet Security: The Effect of Transaction Costs on Managed Service Providers.” International Conference on Telecommunication Systems, Modeling and Analysis, Dallas, TX, November 17-20.

Ding, W. and W. Yurcik (2006). “Economics of Internet Security Outsourcing: Simulation Results Based on the Schneier Model.” Workshop on the Economics of Securing the Information Infrastructure, Washington D.C., October 23-24.

DiRomualdo, A. and Gurbaxani, V. (1998). "Strategic Intent for IT Outsourcing," Sloan Management Review, Summer, pp. 67-80.

Moving Beyond Compliance Ernst & Young's 2008 Global Information Security Survey http://www.ey.com/Global/assets.nsf/UK/Global_Information_Security_Survey_2008/$file/EY_Global_Information_Security_Survey_2008.pdf

Frost & Sullivan, (2003). "World Managed Security Service Provider Markets" #7426-74.

Gal-Or, E. and Ghose, A. (2005). "The Economic Incentives for Sharing Security Information," Information Systems Research. 16(2), pp.186-208.

Gordon, L. A., M. Loeb, W. Lucyshyn. 2003. “Sharing information on computer systems security: An economic analysis,” Journal of Accounting and Public Policy, Vol. 22 No. 6, pp. 461–485.

Gupta, A. and D. Zhdanov (2007). “Growth and Sustainability of Managed Security Services Networks: An Economic Perspective.” Workshop on the Economics of Information Security, Pittsburgh, June 7- 8.

Gurbaxani, V. (2006). "Information Systems Outsourcing Contracts: Theory and Evidence," Managing in the Information Economy: Current Research, (U. Apte, U. Karmarkar, eds), Kluwer.

Hu, Q., Saunders, C., and Gebelt, M.(1997)."Research Report: Diffusion of Information Systems Outsourcing: A Reevaluation of Influence Sources," Information Systems Research, Vol. 8, pp.288-301.

Kavanagh, K. M., Pescatore, J. (2005). "Magic Quadrant for MSSPs, North America, 2H05", Gartner

Kavanagh, K. M., Pescatore, J. (2007). "Magic Quadrant for MSSPs, North America, 1H07", Gartner

Lacity, M. and R. Hirscheim, (1993). “Information Systems, Outsourcing, Myths, Metaphors and Realities,” New York, NY, John Wiley and Sons.

Loh, L., Venkatraman, N. (1992a). "Determinants of Information Technology Outsourcing: A Cross-Sectional Analysis," Journal of Management Information Systems, Vol.9, pp.7-24.

Loh, L., Venkatraman, N. (1992b). "Diffusion of Information Technology Outsourcing: Influence Sources and the Kodak Effect," Information Systems Research, Vol.3, No.4, pp.334-358.

McGuire, Timothy M., Richard P. Staelin (1983), "An industry equilibrium analysis of down-stream vertical integration," Marketing Science, Vol. 2, pp 161192.

McLellan, K. L., Marcolin, B. L. and Beamish, P. W.(1995). "Financial and Strategic Motivations Behind IS Outsourcing," Journal of Information Technology, Vol. 10, pp. 299-321.

Messmer, E., "Outsourcing security tasks brings controversy," Network World, 03/20/2008 http://www.networkworld.com/news/2008/032008-outsourcing-security.html.

Palumbo, S., (2006), Yankee Group Research, "The Managed Security Services Opportunity," http://www.mcafee.com/us/local_content/white_papers/wp_service_provider.pdf.

Ponemon Institute, (2007). "Annual Study: U.S. Cost of a Data Breach Understanding Financial Impact, Customer Turnover, and Preventitive Solutions".

Ponemon Institute, (2007). "Consumer Survey on Data Breach Notification".

Reed, B., May 27, 2008, "Study: Managed services market to crack $66 billion by 2012," http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9089478.

Rowe, B**.** (2007)**,** "Will Outsourcing IT Security Lead to a Higher Social Level of Security?," Workshop on Economics of Information Security 2007.

Sen, S., Raghu, T. S., and Vinze, A., (2009)**,** "Demand Heterogeneity in IT Infrastructure Services: Modeling and Evaluation of a Dynamic Approach to Defining Service Levels," Information Systems Research, Volume 20, No: 2

Slaughter, S. A., Ang, S. (1996). "Employment Outsourcing in Information Systems," Communications of the ACM, Vol. 39, No. 7, pp. 47-54.

Sobol, M. G., and Apte, U. M. (1995). "Domestic and Global Outsourcing Practices of America’s most Effective IS Users," Journal of Information Technology, Vol. 10, pp. 269-280.

Sridhar, S. S., and Balachandran, B. V. (1997). "Incomplete Information, Task Assignment, and Managerial Control Systems," Management Science, Vol. 43, No. 6, pp. 764-778.

Tarantino, A., (2008), "Governance, Risk, and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices." John Wiley & Sons, Hoboken, New Jersey.

Van Mieghem, J.A. (1999), "Coordinating investment, production, and subcontracting," Management Science, Vol. 45 No. 7, pp. 954-71.

Whang, S. (1992)."Contracting for Software Development," Management Science, Vol. 38, pp. 307-324.

Wylder, J. (2004). "Stretegic Information Security," Boca Raton, Florida, Auerbach Publications.

(“National Consumer Survey on Data Security Breach Notification”)

Appendix

Derivation of optimal prices

$\pi_i = p_i \cdot q_i = p_i \cdot (a - b_1 \cdot p_i + b_2 \cdot p_j + B_i)$

$\dfrac{\partial \pi_i}{\partial p_i} = a - 2b_1 \cdot p_i + b_2 \cdot p_j + B_i = 0 \Rightarrow p_i(p_j) = \dfrac{a + b_2 \cdot p_j + B_i}{2b_1}$. This implies that $p_i = \dfrac{q_i}{b_1} \Rightarrow \pi_i = (p_i^*)^2 \cdot b_1$. Solving the reaction functions simultaneously, we obtain the following optimal price.

$$p_i^*(p_j) = \frac{a(2b_1 + b_2) + 2b_1 B_i + b_2 B_j}{4b_1^2 - b_2^2} \; .$$

□

Proof of Lemma 1

To find the game's equilibrium:

When firm *i* outsources, firm *j* outsources if its payoff under outsourcing is higher than its payoff under in-house management, i.e.,

$(\theta^O - P^{OO})(V - L) > (\theta^O - P^{OI})V - (\theta^I - P^{OI})L \Rightarrow \left(\theta^O - \theta^I\right) < (P^{OI} - P^{OO})\left(\dfrac{V - L}{L}\right)$. Replacing $R = \dfrac{V}{L}$,

we get the (outsource, outsource) Nash equilibrium, $\left(\theta^O - \theta^I\right) < (P^{OI} - P^{OO})\left(R - 1\right)$. Similarly, we obtain (in-house, in-house) Nash equilibrium, when (outsource, outsource) is not Nash equilibrium and $\left(\theta^O - \theta^I\right) > \left(R - 1\right)(P^{II} - P^{OI})$ holds, that is $\left(\theta^O - \theta^I\right) > Max\left(\left(R - 1\right)(P^{II} - P^{OI}), \left(R - 1\right)(P^{OI} - P^{OO})\right)$.

When there is no pure strategy, firms outsource with the mixing probability calculated by payoff-equating method.

Proof of Proposition 1 (a)

When there is no speculative risk, i.e., V=$L \Rightarrow R$=1, $\left(\theta^O - \theta^I\right) < (P^{OI} - P^{OO})\left(R - 1\right)$ holds when $\theta^O < \theta^I$, since right hand side of the inequality (RHS) is zero.

Proof of Proposition 1 (b)

When there is speculative risk, after an increase in *R*, regardless of the sign of the left hand of the inequality (LHS), this condition $\left(\theta^{O}-\theta^{I}\right)<(P^{OI}-P^{OO})\left(R-1\right)$ is more likely to satisfied if $P^{OI}>P^{OO}$, since in that case RHS increases. □

Proof of Proposition 2 (a)

An increase in MSSP quality makes LHS of the inequality, $\left(\theta^{O}-\theta^{I}\right)<(P^{OI}-P^{OO})\left(R-1\right)$, lower, hence inequality is more likely to be satisfied. □

Proof of Proposition 2 (b)

When *R*>1, an increase in P^{OO}, reduces the value of RHS of the inequality, $\left(\theta^{O}-\theta^{I}\right)<(P^{OI}-P^{OO})\left(R-1\right)$, and this makes it more difficult to satisfy the inequality. When *R*<1, an increase in P^{OO}, increases the value of RHS of the inequality, and this makes it easier to satisfy the inequality. □

Proof of Proposition 3 (a)

The proof follows from the derivative of R w.r.t. α.

$$\frac{\partial R}{\partial \alpha}=\frac{4b_1(2b_1+b_2)(4(2a-\Delta)(a+\alpha\Delta)b_1^2+2(4a^2-a(5+\alpha^2)\Delta+(2+\alpha+\alpha^2)\Delta^2b_1b_2+(a-\Delta)(2a+\alpha(2+\alpha)\Delta)b_2^2)}{(-2b_1+\alpha b_2)^2((4a-2\Delta)b_1+(2a+\alpha\Delta)b_2)^2}>0$$

since $b_1>b_2$, a≥Δ by assumption. Hence an increase in spillover increases *R* and the rest of the Proposition 4 follows from Proposition 1(ii). □

Proof of Proposition 3 (b)

The proof follows from the derivative of R w.r.t. a.

$$\frac{\partial R}{\partial \Delta}=\frac{4\Delta b_1(1+\alpha)(2b_1+b_2)(2b_1\alpha-(2+\alpha)b_2)}{(2b_1-\alpha b_2)((4a-2\Delta)b_1+(2a+\alpha\Delta)b_2)^2},\ \frac{\partial R}{\partial \Delta}<0\ if\ \alpha<\frac{2b_2}{2b_1-b_2}\ and\ \frac{\partial R}{\partial \Delta}>0\ if\ \alpha>\frac{2b_2}{2b_1-b_2}$$

The rest of the proposition follows from Proposition 1(ii). □

Proof of Proposition 4

When the condition, $(P^{OI}-P^{OO})(R-1)<\left(\theta^{O}-\theta^{I}\right)<(P^{II}-P^{OI})(R-1)$, is satisfied; depending on whether $\theta^{O}<\theta^{I}$ or $\theta^{O}>\theta^{I}$, (*outsource*, *in-house*) or (*in-house*, *outsource*) equilibrium is reached,.

Consider the region where the condition holds. The size of the region increases when *R*>1 and decreases otherwise. See the following examples:

1) $R = 1.5, P^{OI} = 0.2, P^{OO} = 0.4, P^{II} = 0.1 \Rightarrow -0.1 < \theta^{O} - \theta^{I} < -0.05$, after an increases in *R* (*R* =1.7), $-0.14 < \theta^{O} - \theta^{I} < -0.07$, note that the size of the region the condition holds gets larger.

2) $R = 0.5, P^{OI} = 0.2, P^{OO} = 0.4, P^{II} = 0.1 \Rightarrow 0.1 < \theta^{O} - \theta^{I} < 0.05$, after an increases in *R* (*R* =0.7) $0.06 < \theta^{O} - \theta^{I} < 0.03$, note that the size of the region the condition holds gets smaller. □

Proof of Proposition 5 (a)

$(P^{OI} - P^{OO})(R-1) < \left(\theta^{O} - \theta^{I}\right) < (P^{II} - P^{OI})(R-1)$, after an improvement in MSSP quality, the LHS of the inequality is less likely to be satisfied. □

Proof of Proposition 5 (b)

Increase in P^{OO} impacts the LHS of the inequality, $(P^{OI} - P^{OO})(R-1) < \left(\theta^{O} - \theta^{I}\right) < (P^{II} - P^{OI})(R-1)$. When *R*>1, after an increase in P^{OO}, LHS is easier to satisfy and more difficult satisfy otherwise. □